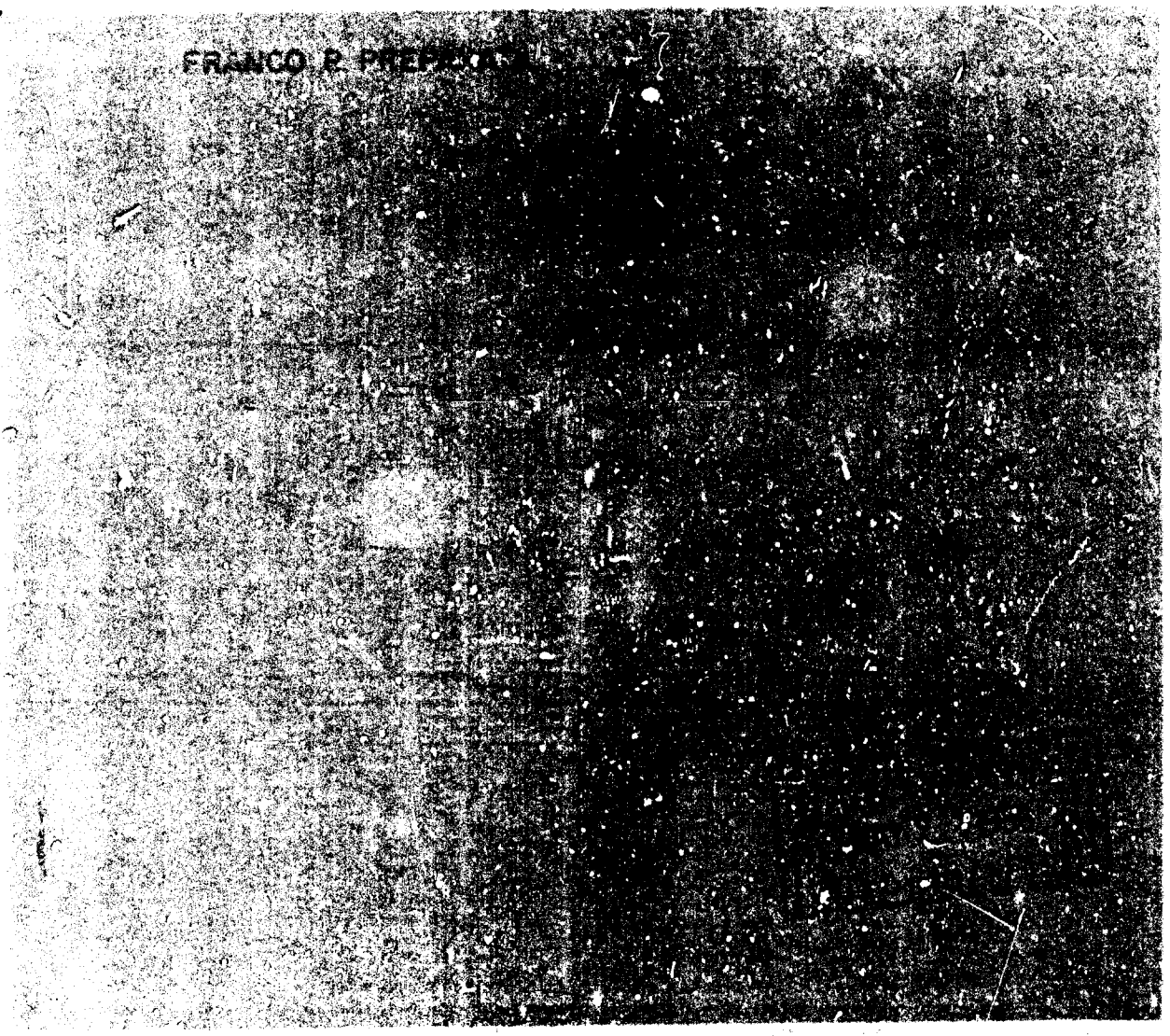
REPORT R-375 APRIL, 1968

COORDINATED SCIENCE LABORATORY

A STUDY OF NORDSTROM-ROBINSON OPTIMUM CODE



UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under contract DAAB-07-67-C-0199; and in part by NSF Grant GK-2339.

A Study of Nordstrom-Robinson Optimum Code*

Franco P. Preparata

Summary

The optimum quadratic (15,8) code with minimum distance d=5, recently discovered and studied by Nordstrom and Robinson, can be rather naturally described in terms of polynomials over GF(2). It is shown that the Nordstrom-Robinson code consists of a linear code and of a certain subset of its cosets, which account for its non-linear nature. This representation leads to a non-heuristic proof that weight and distance structures can be treated analogously and that the minimum distance and weight are 5. The analysis of this mechanism may be an essential step in the discovery of an entire class of non-linear double error correcting codes. The given analysis also suggests a systematic decoding procedure. This is based on permutations which map any correctable error pattern (double or single errors) into digit positions for which the computation of a syndrome allows the correction. The correct code word can then be recovered through the inverse permutation.

1. Introduction

An interesting non-group (15,8) binary code of minimum distance d = 5 has been recently discovered by Nordstrom and Robinson [1,2]. As noted in these references, two non-group codes reported in the past years, i.e., the

*This work was supported in part by the Joint Services Electronics Program under Contract DAAB 07-67-C-0199 and in part by NSF Grant GK 2339. Part of the results reported here were presented at the Second Princeton Conference on Information Sciences and Systems.

codes presented by Nadler [3] and Green [4], have lost their puzzling identity to become subcodes (in the sense of shortened codes) of the Nordstrom-Robinson (NR hereafter) code. The latter is particularly attractive because it is more efficient than the corresponding linear code with the same length and minimum distance, i.e., the BCH (15,7) code.

The purpose of this paper is mainly to present a new description of the NR code in terms of polynomials over GF(2), which may be considered as an additional step in the elucidation of the deep structure of this code. Since to date the NR code is an isolated example, the validity of this investigation may be questioned. The reported analysis, however, reveals a structure which is suggestive of the membership of the NR code in a wider class of non-linear codes. The discovery of this class is certainly a fascinating objective and it is felt that the presented description may guide further research in this direction.

As another interesting feature, the polynomial representation suggests almost naturally a systematic decoding procedure. This procedure is based on a subgroup of the group of permutations for which the NR code is an invariant and on the processing of a syndrome-like function of the received vector.

2. The Polynomial Description

All polynomials considered in the sequel belong to the algebra A of polynomials over GF(2) modulo (x^7+1)[5]. By $\{m(x)\}$ we denote the ideal of polynomials $m(x)$, mod (x^7+1), generated by $g(x) = x^3+x^2+1$, i.e., the (7,4)

hamming code.

Consider now a generic polynomial $i(x) \epsilon A$, i.e., a polynomial of degree < 7. Clearly i(x) belongs either to $\{m(x)\}$ or to one of its cosets. If we take as coset leaders of $\{m(x)\}$ the minimum weight polynomials q(x) in the coset, i(x) admits of a unique decomposition

$$i(x) = m(x)+q(x) \tag{1}$$

where $m(x) \epsilon \{m(x)\}$ and q(x) is a coset leader of $\{m(x)\}$. Since a Hamming code is a perfect code, q(x) is of the form ax^{α}, where a = 0,1 and α = 0,1, ...,6; moreover, q(x) is readily found by multiplying i(x) by the polynomial $f(x) = x^6+x^5+x^3+1$, which belongs to the dual code of $\{m(x)\}$. Due to the fact that f(x) is a maximum length sequence, we have

$$i(x)f(x) = \begin{cases} 0 & \rightarrow a=0 \\ x^j F(x) & \rightarrow a=1,\ \alpha=j \end{cases}$$

Once q(x) has been found, m(x) = i(x)+q(x) and decomposition (1) is obtained.

Given two polynomials a(x) and b(x) in the algebra A and a binary constant i_7, we form 15-component vectors over GF(2) of the form

$$\underline{w} = [a(x),\ i_7,\ b(x)] \tag{2}$$

With this notation we mean that the 7 rightmost (leftmost) components of $\underline{w}$ are given by the ordered sequence of the coefficients of b(x) (of a(x)). Let us now construct vectors of the form

$$\underline{w} = [i(x),\ i_7,\ m(x) + i(x)f(x) + bu(x)] \tag{3}$$

where $u(x) = (x^7+1)/(x+1) = x^6+x^5+x^4+x^3+x^2+x+1$ and b is the parity of the

Hamming weight of the 8-component vector $[m(x), i_7]$. We claim that all vectors given by (3), for any arbitrary choice of $i(x)$ and i_7, constitute the NR code (apart from the minor difference that in [1] and [2] $i(x)$ is replaced by $x^6 i(x)$, i.e., a one-position cyclic shift of $i(x)$).

In fact let

$$m(x)+i(x)f(x)+bu(x) = r(x) = \sum_{j=0}^{6} r_j x^j$$

$$i(x) = \sum_{j=0}^{6} i_j x^j$$

$$m(x) = \sum_{j=0}^{6} m_j x^j$$

To obtain $m(x)$ we must first know $q(x)$. To this end let

$$i(x).f(x) = \Sigma p_j x^j$$

If $q(x) = 0$, then $p_j = 0$ for every j. If $q(x) = x^\alpha$, then $p_\alpha p_{\alpha-1} p_{\alpha-2} = 1$ while $p_k p_{k-1} p_{k-2} = 0$ for $k \neq \alpha$ (all the subscripts are intended modulo 7). It follows that

$$m(x) = i(x)+q(x) = i(x)+\sum_{j=0}^{6} p_j p_{j-1} p_{j-2} x^j = \sum_{j=0}^{6} (i_j+p_j p_{j-1} p_{j-2}) x^j$$

i.e.,

$$m_j = i_j+p_j p_{j-1} p_{j-2} \qquad (4)$$

From the definition of $r(x)$ we obtain

$$\sum_{j=0}^{6} r_j x^j = \sum_{j=0}^{6} m_j x^j + \sum_{j=0}^{6} p_j x^j + \sum_{j=0}^{6} \left(\sum_{k=0}^{6} m_k + i_7 \right) x^j$$

or, equivalently,

$$r_j = m_j + p_j + \sum_{k=0}^{6} m_k + i_7 \qquad (5)$$

Recalling now that

$$p_j = i_j + i_{j+1} + i_{j+2} + i_{j+4}$$

substituting (4) into (5) we obtain, after considerable and unrewarding manipulations,

$$r_j = i_7 + i_j + i_{j+1} + i_{j+2} + i_{j+4} \qquad (5')$$
$$+(i_{j+1}+i_{j+5})(i_{j+2}+i_{j+3})+(i_{j+1}+i_{j+5})(i_{j+4}+i_{j+6})$$
$$+(i_{j+2}+i_{j+3})(i_{j+4}+i_{j+6})$$

which, except for the slight difference mentioned earlier, coincides with the expression obtained by Robinson.

We now rewrite relation (3) as

$$\underline{w} = [m(x)+q(x),\ i_7,\ m(x)+q(x)f(x)+bu(x)]$$

Clearly $\underline{w}$ can be expressed as

$$\underline{w} = \underline{v} + \underline{u} \qquad (6)$$

with

$$\underline{v} = [m(x),\ i_7,\ m(x)+bu(x)] \qquad (7)$$

$$\underline{u} = [q(x),\ 0,\ q(x)f(x)] \qquad (8)$$

Inspection of (7) shows that all vectors $\underline{v}$, obtained for an arbitrary choice of $m(x) \in \{m(x)\}$, form a linear code: specifically, it is easy to recognize its equivalence to the (15,5) triple-error correcting BCH code. For brevity we shall refer to this code as to the "kernel." It is also clear that,

since $q(x) \neq 0$ is a coset leader of $\{m(x)\}$, distinct vectors $\underline{u} = [q(x),0,q(x)f(x)]$ identify cosets of the kernel. Recalling that $q(x) = ax^{\alpha}(a=0,1)(\alpha=0,1,\ldots,6)$ we have the following interesting interpretation of the NR code: the NR code consists of the code words of the kernel and of its seven cosets identified by distinct $\underline{u}$'s for which $q(x) \neq 0$.

3. Weight and Distance Structure

By $W[a(x)]$ we denote the number of nonzero coefficients of $a(x)$. The Hamming distance between two polynomials $a(x)$ and $b(x)$, denoted by $d[a(x), b(x)]$ is clearly

$$d[a(x), b(x)] = W[a(x)+b(x)]$$

We now give two preparatory lemmas.

Lemma 1. - The polynomial $q(x)+f(x)q(x)$ belongs to $\{M(x)\}$ and

$$W[q(x)+f(x)q(x)] = \begin{cases} 0 & \leftarrow \quad q(x) = 0 \\ 3 & \leftarrow \quad q(x) \neq 0 \end{cases}$$

Proof: We notice that the polynomial $f(x)$ enjoys the property

$$f^2(x) = f(x)$$

From this we immediately derive

$$f(x)\{q(x)+f(x)q(x)\} = f(x)q(x)+f^2(x)q(x) = 0$$

i.e., $q(x)+f(x)q(x) \in \{m(x)\}$, being orthogonal to $f(x)$. Moreover, if $q(x) = 0$, then $q(x)+f(x)q(x) = 0$ and obviously $W[q(x)+f(x)q(x)] = 0$. If $q(x) \neq 0$, then $W[q(x)] = 1$. From $W[f(x)q(x)] = 4$ it follows that $W[q(x)+q(x)f(x)] = 3$.

Q.E.D.

Lemma 2. - The sum of two vectors $\underline{u}_1$ and $\underline{u}_2$ of the form (8) admits of the representation

$$\underline{u}_1+\underline{u}_2 = \underline{v}'+\underline{q}+\underline{p} \tag{9}$$

with $$\underline{v}' = [m'(x),0,m'(x)+bu(x)] \quad , \quad m'(x)\in\{m(x)\} \tag{10}$$

$$\underline{q} = [q(x),0,q(x)] \tag{11}$$

$$p = [0,0,m''(x)] \quad , \quad m''(x)\in\{m(x)\} \tag{12}$$

Moreover $W[m'(x)] = 0,3$. If $q(x) \neq 0$,

$$W[m''(x)] = 3 \tag{13a}$$

$$W[m''(x)+q(x)] = 4 \tag{13b}$$

Proof: Let $\underline{u}_1 = [q_1(x),0,f(x)q_1(x)]$ and $\underline{u}_2 = [q_2(x),0,f(x)q_2(x)]$. Then their sum is

$$\underline{u}_1+\underline{u}_2 = \left[q_1(x)+q_2(x),0,f(x)\left(q_1(x)+q_2(x)\right)\right]. \tag{14}$$

Decomposition (1) can be applied to $q_1(x)+q_2(x)$, i.e.,

$$q_1(x)+q_2(x) = m'(x)+q(x)$$

From this we have

$$m'(x) = q_1(x)+q_2(x)+q(x) \tag{15}$$

which shows that $W[m'(x)] = 3$ if and only if $q_1(x) \neq q_2(x)$, $q_1(x) \neq 0$, $q_2(x) \neq 0$, and is 0 otherwise. Relation (14) can now be rewritten as

$$\underline{u}_1+\underline{u}_2 = \left[m'(x)+q(x),0,\left(m'(x)+bu(x)\right)+q(x)+q(x)+f(x)q(x)+m'(x)+bu(x)\right]$$

$$= \left[m'(x),0,m'(x)+bu(x)\right]+\left[0,0,q(x)+f(x)q(x)+m'(x)+bu(x)\right]$$

$$+\left[q(x),0,q(x)\right]$$

where b is chosen according to the rule

$$b = \begin{cases} 0 \text{ if } W[m'(x)] = 0 \\ 1 \text{ if } W[m'(x)] = 3 \end{cases}$$

To prove (9), all we need to show is that

$$m''(x) = q(x)+f(x)q(x)+m'(x)+bu(x) \qquad (16)$$

belongs to $\{m(x)\}$. But this follows immediately, since the three polynomials $m'(x)$, $u(x)$, $q(x) + f(x)q(x)$ belong to $\{m(x)\}$.

To prove (13a,b), assume first that $m'(x) = 0$. Then (16) becomes $m''(x) = q(x)+f(x)q(x)$ and (13a) follows from Prop. 1. Furthermore $W[m''(x)+q(x)] = W[f(x)q(x)] = 4$ and (13b) is proved. Assume now that $m'(x) \neq 0$. Denoting $q(x)$ by x^k, relation (16) becomes (b=1)

$$m''(x) = x^k(1+f(x))+m'(x)+u(x).$$

We notice that the coefficient of x^k is 0 in $x^k(1+f(x))$ and is 1 both in $u(x)$ and in $m'(x)$ (see relation (15)). This has the following consequences: i) $m'(x) \neq x^k(1+f(x))$. From $W[m'(x)] = 3$, $W[x^k(1+f(x))] = 3$ we then obtain $W[m'(x)+x^k(1+f(x))] = 4$ and $W[m''(x)] = 3$; ii) the coefficient of x^k in $m''(x)$ is 0. Hence

$$W[m''(x)+q(x)] = W[m''(x)]+W[q(x)] = 4.$$

Q.E.D.

We can now prove the following theorem.

Theorem 1. - Given any two distinct code words $\underline{w}_1$ and $\underline{w}_2$ of the NR code, their Hamming distance is never less than 5.

Proof: Let $\underline{w}_1 = \underline{v}_1+\underline{u}_1$ and $\underline{w}_2 = \underline{v}_2+\underline{u}_2$. Then, using (9), we obtain

$$\underline{w}_1+\underline{w}_2 = (\underline{v}_1+\underline{v}_2)+(\underline{u}_1+\underline{u}_2) = (\underline{v}_1+\underline{v}_2+\underline{v}')+\underline{p}+\underline{q}$$

or

$$\underline{w}_1+\underline{w}_2 = \underline{v}+\underline{p}+\underline{q} \tag{17}$$

where we have set $\underline{v} \triangleq \underline{v}_1+\underline{v}_2+\underline{v}'$. Clearly $\underline{v}$ is an arbitrary member of the kernel and $\underline{p}$, $\underline{q}$ are defined by relations (11),(12),(13a),(13b). If $\underline{q} = [0,0,0]$, clearly $\underline{u}_1 = \underline{u}_2$ and $(\underline{w}_1+\underline{w}_2)$ belongs to the kernel: since the minimum weight of the code words of the kernel is 7, the assertion is proved.

Assume now that $\underline{q} \neq [0,0,0]$. Let W denote the weight of $(\underline{w}_1+\underline{w}_2)$. If $\underline{v} = [0,0,0]$ then

$$W = \text{weight}[q(x),0,q(x)+m''(x)]$$
$$= W[q(x)]+W[q(x)+m''(x)] = 1+4 = 5$$

which follows from (11b) and $W[q(x)] = 1$. If $\underline{v} \neq [0,0,0]$ consider the sum

$$\underline{s} = \underline{v}+\underline{p} = [m(x),\ i_7,\ m(x)+bu(x)+m''(x)]$$

Clearly $\underline{w}_1+\underline{w}_2 = \underline{s}+\underline{q}$ and

$$W = i_7+d[m(x),q(x)]+d[m(x)+m''(x)+bu(x),q(x)] \tag{18}$$

Since $q(x) \notin \{m(x)\}$, $q(x)$ is distinct from both $m(x)$ and $[m(x)+m''(x)+bu(x)]$. It follows that the triangle inequality applies strictly, i.e.,

$$d[m(x),q(x)]+d[m(x)+m''(x)+bu(x),q(x)] >$$
$$> d[m(x),m(x)+m''(x)+bu(x)] = W[m''(x)+bu(x)]$$

Relation (18) becomes therefore

$$W > i_7+W[m''(x)+bu(x)] \tag{18a}$$

Depending upon the value of b we distinguish two cases:

A) b=1. From (13a), $W[m''(x)]=3$, we have $W[m''(x)+u(x)]=4$ and (18a) yields $W > 4$ (i.e. $W \geq 5$).

B) b=0. If $i_7 = 1$, relation (18a) yields $W > 1+W[m''(x)] = 4$ and we still have $W \geq 5$. We now remark that b=0, $i_7=0$, $m(x)\neq 0$ imply $W[m(x)] = 4$.

Then by using equations (10), (11) and (12) we have

$$W = W[m(x)+q(x)]+W[m(x)+m''(x)+q(x)]$$

Now $W[m(x)+q(x)]\geq W[m(x)]-W[q(x)]=4-1=3$. Similarly $W[m(x)+m''(x)+q(x)]\geq W[m(x)+m''(x)]-W[q(x)]$. But $W[M(x)]=4$ and $W[m''(x)]=3$ imply that $W[m(x)+m''(x)]$ be odd, i.e., $W[m(x)+m''(x)] \geq 3$. It then follows that $W \geq 3+2 = 5$.

Q.E.D.

Finally, we like to investigate the weight structure of the NR code. The task is extremely simplified by the following lemma which results immediately from (6) and (8).

Lemma 3. - Any code word $\underline{w}$ of the NR code admits of the following decomposition

$$\underline{w} = \underline{v}+\underline{q}+\underline{p}' \qquad (19)$$

where $\underline{v}$ is a member of the kernel, $\underline{q}$ is given by (11), and $\underline{p}'=[0, 0q(x)+f(x)q(x)]$.

We now remark that the vector $\underline{p}'$ of (19) is analogous to the vector $\underline{p}$ of (12). In fact $m^*(x) \triangleq q(x)+f(x)q(x)$ belongs to $\{m(x)\}$ and if $q(x) \neq 0$, lemma 1 yields: $W[m^*(x)] = 3$ and $W[q(x)+m^*(x)] = 4$. We see therefore that

by an argument exactly parallel to the one used to prove theorem 1 we can demonstrate the following assertion:

Theorem 2. - The NR code has minimum weight 5.

This concludes the formal justification of the acute heuristic observation of Nordstrom and Robinson.

4. A Decoding Procedure

The polynomial description given in Section 2 also leads to a decoding algorithm of the NR code, which differs in an essential step from the one described in [2], i.e., the permutation for the convenient positioning of the error pattern to be corrected.

We represent the error pattern as a vector (whose total weight does not exceed 2 for correctability)

$$\underline{e} = [e_1(x), e_7, e_2(x)]$$

with obvious significance of the symbols. Further, we let $R[i(x), i_7] = r(x)$, namely, R denotes the operation of computing the redundant digits r_j ($j=0,1,\ldots,6$) as prescribed by (5'). We now compute the polynomial

$$\tau(x) = R[i(x)+e_1(x), i_7+e_7]+r(x)+e_2(x) \qquad (20)$$

which coincides with the pseudo-syndrome mentioned in [2].

Let us now assume that $e_1(x) = 0$. In this hypothesis we obtain

$$\begin{aligned}\tau(x) &= R[i(x), i_7+e_7]+r(x)+e_2(x)\\ &= m(x)+i(x)f(x)+(b+e_7)u(x)+m(x)+i(x)f(x)+bu(x)+e_2(x)\\ &= e_7u(x)+e_2(x)\end{aligned}$$

With reference to the number W of nonzero coefficients of $\tau(x)$(the weight of $\tau(x)$) and recalling that the weight of $[e_7,e_2(x)]$ cannot exceed 2, we distinguish the following cases:

1. W=0. This implies $e_7=0$, $e_2(x)=0$, i.e., the received vector is error-free.

2. W=1,2. This implies $e_7=0$, $e_2(x)=\tau(x)$.

3. W=6,7. This implies $e_7=1$, $e_2(x)=\tau(x)+u(x)$.

We stress that if $e_1(x) = 0$, W cannot take any other value than 0,1,2,6,7. The converse is also true. For, assume that W = {0,1,2,6,7}. According to the previous discussion we can form e_7', $e_2'(x)$ (the prime denotes that these are estimated error patterns, not the actual ones). Then we add $[0,e_7',e_2'(x)]$ to the received vector and obtain

$$\underline{w}' = [i(x)+e_1(x),\ i_7+e_7+e_7',\ r(x)+e_2(x)+e_2'(x)].$$

From the definition of $\tau(x)$ we compute

$$\tau(x) = R[i(x)+e_1(x),\ i_7+e_7+e_7']+r(x)+e_2(x)+e_2'(x) = 0$$

i.e., $\underline{w}'$ is a code word. Since the distance of w from the received vector cannot exceed 2, from the distance property of the code (d=5) we conclude that $\underline{w}'$ is the correct output. Decoding is therefore easily accomplished whenever $\tau(x)$ = {0,1,2,6,7} or, equivalently, whenever the i(x)-positions are error-free.

Our decoding problem is not yet solved when $e_1(x) \neq 0$. Should we find, however, an artifice which reduces any error pattern to the $e_1(x) = 0$ condition, by "mapping" the error pattern into the $[i_7,r(x)]$-positions, a

solution would be obtained. This artifice is the group {P} of permutations of 15 elements with respect to which the NR code is an invariant, that is, a permutation P belongs to {P} ii and only if, for a code word $\underline{w}_1$, $P\underline{w}_1 = \underline{w}_2$ is also a code word. To gain some insight into the structure of this group, we recall (as noted in [2]) that the NR code is a subset of an (15,11) Hamming code. In fact

$$\{f(x)+u(x)\}\ \{f(x)i(x)+i_7u(x)+r(x)\} = 0$$

since $f(x)u(x) = 0$, $f(x)m(x) = 0$, $u^2(x) = u(x)$. If this expression is translated into matrix form, we obtain a 7X15 matrix A premultiplying the column vector $\underline{w}^T$.[1] Only four rows of the matrix A are linearly independent, i.e.,

$$H = \begin{bmatrix} 0&1&0&0&1&1&1&1&1&0&1&1&0&0&0 \\ 1&1&1&0&1&0&0&0&1&1&1&0&1&0&0 \\ 0&0&1&1&1&0&1&1&1&1&0&0&0&1&0 \\ 1&0&0&1&1&1&0&1&0&1&1&0&0&0&1 \end{bmatrix}$$

which shows that each word $\underline{w}$ of the NR code is necessarily in the null space of H, the parity check matrix of the (15,11) Hamming code.

It follows that {P} is contained in the group {Q} for which the Hamming (15,11) code is an invariant. This group {Q} can be easily found. Given any permutation Q, the relation

$$QH^T = H^TB \tag{21}$$

tells us that H^TB must be column equivalent to H^T, i.e., B must be a nonsingular 4X4 matrix. The converse is also true. In fact, given any nonsingular B, since all the rows of H^T are distinct, no two rows of H^TB are equal: hence there exists a permutation Q which maps H^T into H^TB. The group

[1] If A is a matrix, A^T is its transpose.

{Q} is therefore isomorphic to the group of 4x4 nonsingular matrices: the order of this group is clearly 15x14x12x8. It can also be shown that the kernel, as defined in section 2, is invariant with respect to {Q}. If we now recall relations (6,), (7), and (8) we have that for any P∈{P}, since P∈{Q} also, P$\underline{v}$ belongs to the kernel. We must therefore insure that for every $\underline{u}$ of the form (8)

$$P\underline{u} = \underline{v}+\underline{u}' \tag{22}$$

where $\underline{v}$ belongs to the kernel and $\underline{u}'$ is of the form (8). Relations (21) and (22) completely define the members of {P}.[2]

Two non trivial members of {P} are given below. They are

P_1 = (4, 11, 10, 13, 6, 9, 7, 2, 5, 15, 8, 12, 1, 14, 3)

P_2 = (1, 7, 10, 14, 12, 5, 11, 8, 9, 15, 2, 6, 4, 13, 3)

and generate a group of order 12, as can be readily checked. It is particularly instructive to consider the "transition diagram" of a permutation, i.e., the directed graph associated with a permutation matrix P. In figure 1, solid lines describe the transition diagram of P_1, dotted lines that of P_2. Double-circled nodes identify the $[i_7,r(x)]$-positions. These are referred to as "final".

---

[2]After this paper was written, Dr. J. P. Robinson, of the University of Iowa, conducted a computer search and found that {P} contains 15x14x12 members. This indicates that once three columns of B are assigned, the fourth is completely determined (private communication, Jan. '68).

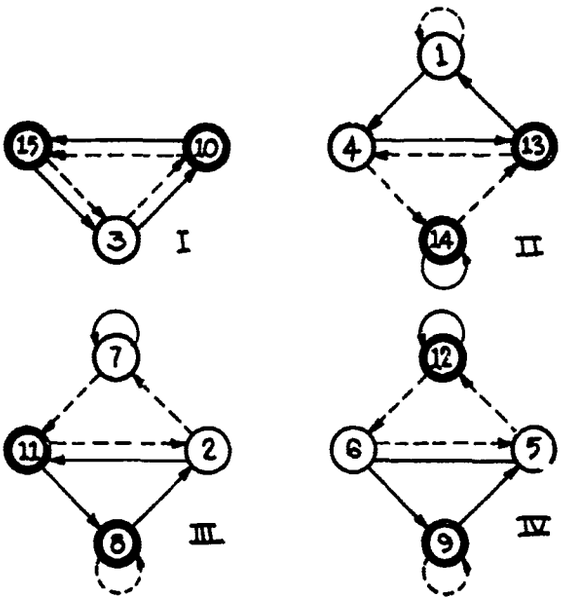


Fig. 1. The combined transition diagrams of P_1 and P_2 (four subdiagrams).

Since each of the four subdiagrams contains final nodes, there is a sequence of the permutations P_1 and P_2 (a P-sequence) which maps any node into a final node. We also claim that any pair of nodes can be mapped into a pair of final nodes. Each of the subdiagrams II, III, IV contains a self-looping final node. Assume that a node of the given pair belongs, say, to II (a similar argument holds for subdiagrams III or IV): then there exists a P-sequence which maps it into node 14. At this point, if the other node has been transformed into 7, the mapping is accomplished by P_2, otherwise by an appropriate sequence of P_1. Finally, when the pair is entirely contained in subdiagram I, the assertion is immediately verified.

The previous argument shows that the group generated by P_1 and P_2 is the device sought. It is now possible to construct a P-sequence $S_{12}S_{11}\cdots S_1(S_j = \{P_1,P_2\})$ which successively generates the 12 members of this group. With the help of the multiplication table, which is omitted for brevity, one such P-sequence is found to be

$$P_2P_2P_1P_1P_2P_1P_2P_2P_2P_1P_1P_2P_1$$

where the rightmost permutation is performed first. The identity permutation is produced at the completion of this P-sequence.

The preceding discussion is recapitulated by the following decoding algorithm:

1.-Set j=0.

2.-Compute $\tau(x)$. If $W = \{0,1,2,6,7\}$ obtain the estimated error pattern and add it to the permuted received vector; else proceed.

3.-If j=12, decoding is complete. If $j\neq 12$ replace j with j+1 and perform S_j on the permuted received vector. Return to Step 2.

This algorithm, although very simple when the number of statements is considered, is susceptible of several further simplifications. Typically once $W = \{0,1,2,6,7\}$ has been found, and the correction has been performed, there is no need for proceeding through the sequence S of permutations. All that is needed is the recovery of the original vector. Specifically if P is the permutation currently applied to the received vector, we must subject the corrected vector to P^{-1}. Inspection of the multiplication table of the group reveals that P^{-1} consists of a P-sequence of length at most 4 (homing

sequence). Hence, once the correction is performed the appropriate homing sequence of permutations could be executed and decoding would be accomplished.

5. Acknowledgment

The author is greatly indebted to Dr. John P. Robinson for a stimulating conversation and for kindly supplying the preprints of his papers.

References

[1] A. W. Nordstrom and J. P. Robinson, "An Optimum Non-linear Code," to appear in Information and Control.

[2] J. P. Robinson, "Analysis of Nordstrom Optimum Quadratic Code," 1st Hawaii International Conference in Systems Sciences, Jan. 1968.

[3] M. Nadler, Topics in Engineering Logic, McMillan, New York, 1962.

[4] M. W. Green, "Two Heuristic Techniques for Block-Code Construction," IEEE Trans. on Information Theory, Vol. IT-12, p. 273, April 1966.

[5] W. W. Peterson, Error Correcting Codes, The M.I.T. Press and J. Wiley & Sons, 1961.

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

A STUDY OF NORDSTROM-ROBINSON OPTIMUM CODE

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

5. AUTHOR(S) *(First name, middle initial, last name)*

Preparata, Franco P.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
April 1968	17	5

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
DAAB-07-67-C-0199; also in part NSF GK-2339 b. PROJECT NO.	R-375
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	

10. DISTRIBUTION STATEMENT

Distribution of this report is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Joint Services Electronics Program thru U.S. Army Electronics Command Ft. Monmouth, New Jersey 07703

13. ABSTRACT

The optimum quadratic (15,8) code with minimum distance d=5, recently discovered and studied by Nordstrom and Robinson, can be rather naturally described in terms of polynomials over GF(2). It is shown that the Nordstrom-Robinson code consists of a linear code and of a certain subset of its cosets, which account for its non-linear nature. This representation leads to a non-heuristic proof that weight and distance structures can be treated analogously and that the minimum distance and weight are 5. The analysis of this mechanism may be an essential step in the discovery of an entire class of non-linear double error correcting codes. The given analysis also suggests a systematic decoding procedure. This is based on permutations which map any correctable error pattern (double or single errors) into digit positions for which the computation of a syndrome allows the correction. The correct code word can then be recovered through the inverse permutation.

DD FORM 1 NOV 68 1473 (PAGE 1)

S/N 0101-807-6811

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Non-linear codes						
Hamming weight						
Hamming distance						
Decoding						
Polynomial codes						